Threat Advisory Services
MALWARE ANALYSIS SERVICE OVERVIEW

Introduction

Escalating malware attacks are a major threat to organizations of every size. Their ability to infiltrate systems, steal sensitive data, disrupt operations, and irrevocably damage brand reputations poses a serious challenge that must be addressed. However, overburdened in-house security teams often lack the time, resources and expertise needed for focused malware analysis to effectively stay ahead of malicious campaigns and attacks.

By outsourcing malware analysis to a trusted services provider, organizations can:

- **Optimize resource allocation:** Strategically allocate resources, ensuring investments in tools, personnel and infrastructure align with organizational priorities.
- **Enhance existing investments:** Collect and deploy indicators of compromise (IOCs) across existing security infrastructure to better identify and mitigate malware exploits.
- **Streamline security operations:** Implement processes and tools to reduce complexity and enhance efficiency across cybersecurity frameworks.
- **Gain access to specialized expertise:** Tap into a dedicated team of analysts to conduct in-depth investigations that identify potentially malicious software, hashes and URLs.

MALWARE ANALYSIS SERVICE

Appgate's Malware Analysis Service, directed by our experienced Malware Analysis and Research Team (MART), features two service offerings that security teams can utilize to submit potentially malicious files, hashes and URLs for investigation. Rapid Analysis uses automated processes, tools and systems to extract data and create a timely, informed report. Deep Analysis leverages industry-leading data sources augmented by in-house methodologies and hands-on, reverse engineering assessments to deliver in-depth insights into more obscure and emerging malware strains.

Both services include actionable IOCs, insights and recommendations with alert levels so security teams can effectively mitigate risks. Organizations also can gain rich contextual threat intelligence for any suspicious indicator derived from submitted samples to proactively enhance incident response efficacy.

MALWARE ANALYSIS SERVICE SUBSCRIPTIONS

Rapid Analysis: This service automatically analyzes known malware sample submissions. The report will include a dedicated section with information such filename, hashes, timestamps, filetype, Command-and-Control (C2) servers, useful strings, images and more. Rapid Analysis reports for most malware samples are delivered within 30 minutes.

Rapid Analysis is recommended as an initial first step for faster service delivery and expedited analysis that includes:

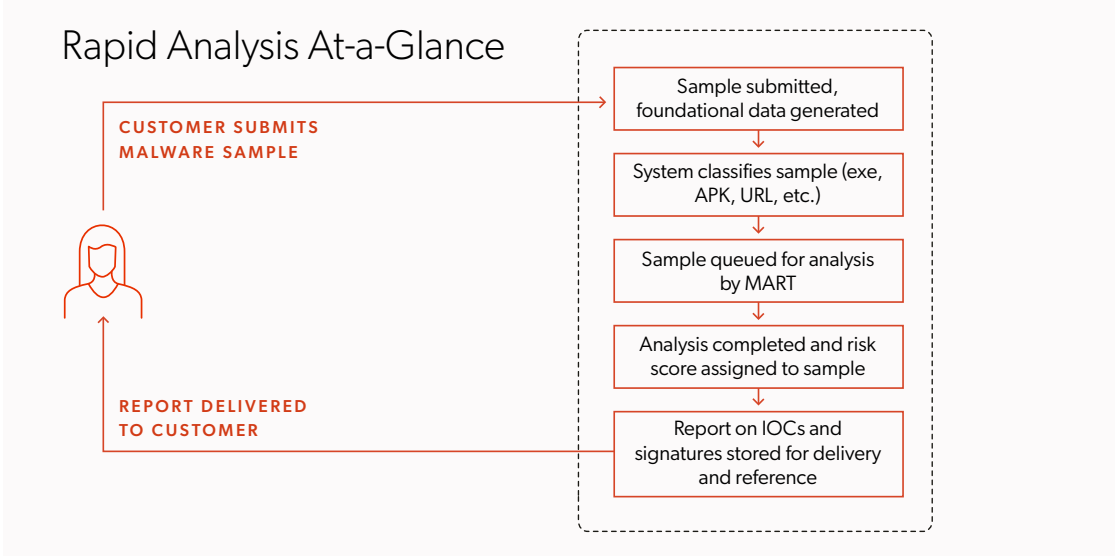
- File ingestion via UI or API
- Static and dynamic analysis
- Rule- and signatures-based identification
- Threat intelligence and IOC reports
- Detection of targeted brands

USE CASES

- **Rapid defense, proactive containment:** Quickly implement identified IOCs into security architecture to proactively contain threats and minimize the blast radius.
- **Security operations:** Integrate the service into existing security operations workflows to enhance threat detection and response capabilities.
- **Malware research:** Conduct in-depth analyses on new and emerging malware samples to understand their behavior and potential impact.
- **Threat hunting:** Proactively search for signs of compromise or emerging threats within enterprise networks or systems.

CRITICAL CAPABILITIES

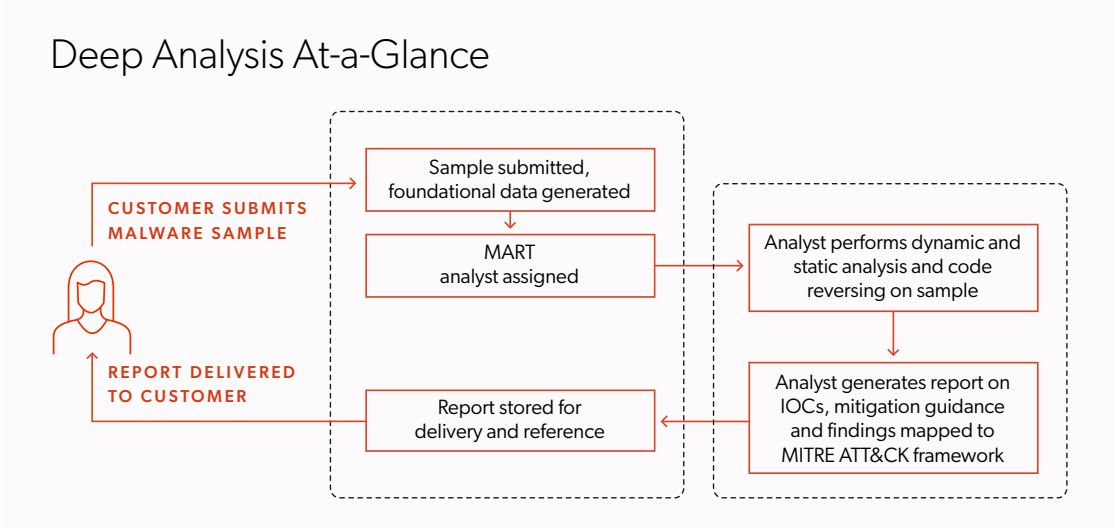
- **Rich contextual threat intelligence:** Leverage advanced reverse engineering methodologies and file and URL analyses to identify malware strains and families and potential impact.
- **Comprehensive reporting:** Generate customized reports according to specific organizational requirements (available in PDF or JSON formats).
- **MITRE ATT&CK mapping:** Map findings to common tactics, techniques and procedures (TTPs) used in advanced persistent threats to develop more effective defense strategies.
- **Practical implementation:** Obtain user-friendly reports and practical recommendations for implementation in existing enterprise security tools and technologies.
- **Compliance support:** Uphold stringent internal policies and regulatory compliance requirements involving malware analysis and incident response.



Deep Analysis: For this service, our Malware Analysis and Research Team reverse engineers malware to uncover customer-specific attack details. The team meticulously analyzes communication with C2 servers and pinpoints malware functions like process injection, web injections and cryptography. A detailed Deep Analysis report provides comprehensive insights including threat behavior and TTPs and is typically delivered in one to three days based on the complexity of the submitted sample.

Deep Analysis is optimal for obscure and emerging malware types that require deeper scrutiny and includes:

- Scope of the malware, its impact and associated family
- Requested permissions
- Behavioral analysis of the sample, injected scripts and functions
- Custom command execution
- C2 investigation
- Full listing of decrypted and relevant strings to denote malware's capabilities
- Addressing customer-specific requirements and specifications



The Four Stages of MART's Deep Analysis

Appgate navigates the intricate landscape of malware analysis through four pivotal stages:

Stage 1: Static analysis — Encompasses review of code strings, hashes, header details and metadata within submitted malware files. Analysis of static properties offers quick risk reduction insights to avoid executing potentially harmful code.

Stage 2: Dynamic analysis — Leverages sandbox environment to execute suspected malicious code. The results allow your security team to closely observe malware behaviors and collect data without risking system or network infection.

Stage 3: Code reversing — If necessary, specialized hands-on analyst investigation into the inner workings of discovered malware including code reversal to uncover hidden functionality, encryption techniques and anti-analysis strategies.

Stage 4: Reporting — A comprehensive report on capabilities and potential effects of the malware. It includes technical details, indicators of compromise (IOCs), detection and mitigation recommendations, and mapping of findings to the MITRE ATT&CK framework.

Benefits

- **Harness our expertise:** Gain access to Appgate's Malware Analysis and Research Team to stay ahead of the latest fraud and cyberthreat trends.
- **Enhance security operations efficiencies:** Streamline security operations and optimize resource allocation to focus on high-priority tasks and strategic initiatives.
- **Improve incident response:** Enrich security telemetry data with threat intelligence to enable faster, more effective mitigation of security incidents.
- **Enhance security posture:** Mitigate the threat of new and emerging strains of malware and suspicious sites with broad platform coverage across Windows, Linux, MacOS and Android.
- **Strong return on investment:** Eliminate the need to dedicate in-house resources to manual analysis and minimize risks associated with potential data breaches and operational disruptions.

Conclusion

Appgate's Malware Analysis Service provides comprehensive, customized and practical mitigation guidance to address evolving malware threats. By leveraging specialized expertise and cutting-edge analysis techniques, organizations can streamline security operations, optimize resource allocation, augment existing tools and technologies, and ensure continuous protection against evolving cyberthreats.

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com

appgate